J.L. Oliveira, P. Gonçalves, W. Dziunikowski, J. Wszolek, S. Rasmussen, R. Lopes, V. Roque
Policy-Based Network Management in an Integrated Mobile Network
IEEE
Pag. 59-64
Digital Object Identifier : 10.1109/AICT.2005.74
ISBN:0-7695-2388-9
http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?asf_arn=null&asf_iid=null&asf_pun=10175&asf_in=null&asf_ rpp=null&asf_iv=null&asf_sp=null&asf_pn=2

Policy-Based Network Management in an Integrated Mobile Network

José Luís Oliveira[1], Pedro Gonçalves[1], Wojciech Dziunikowski[2], Jacek Wszolek[2]
Sonny Rasmussen[3], Rui P. Lopes[4], Vítor Roque[5]
[1]University of Aveiro, DET/IT, Portugal
[2]AGH University of Science and Technology, Poland
[3]UHC, Denmark
[4] Bragança Polytechnic Institute, ESTiG, Portugal
[5] Guarda Polytechnic Institute, ESTG, Portugal
{jlo@det.ua.pt}

Abstract

Through the seamless integration of different kinds of technologies, services and terminals, and with the expected offered bandwidth, the next generation networks will put a new set of challenges related to operation and management. In this paper we present a Policy-based Network Management System that is being developed inside the Daidalos IST project.

1. Introduction

The increasing dependency of citizens on telecommunications resources is pushing even more current technological challenges. While 3G adoption is still in its infancy, Telco's industry is already moving its interest into the next generation networks. The high bandwidth that is expected, the global roaming across multiple networks – wireless, mobile, cellular network, satellite-based or fixed LAN –, and the increase of the number of users and terminals will demand for a redesign of architectures, from the infrastructure physical layer to the topmost business process layer.

However, the rapid technological and societal changes and the emergence of numerous new services have created a complex environment for network operators and a confusing situation for end users. The enhancement of existing technologies and development of new 4G systems will increase this complexity even more. In this context, the network and the system management is a crucial factor in the success of offering new services.

This paper presents the ongoing work that has been done inside the Daidalos project especially concerning management aspects and the strategy to follow a policy-based network management (PBNM) approach.

2. Policy Based Network Management

Today, the main goal of designing a new network management system is to cover all management levels i.e. business, service, network and element in a consistent manner. The sole element management presented by SNMP/MIBs solution is insufficient. Therefore, network should be treated as a large distributed system and not as individual devices. The challenge is to create a high level management rules – policies – and to enforce its execution in the whole network.

In this context we envisage two main architectures, despite several similarities among both: IETF and DMTF. The IETF has proposed a policy framework

architecture with a new information model and new protocols [1]. The MIB concept was replaced by PIB (police information base), several protocols were specified, such as the Common Open Policy Service (COPS) [1] and SNMP for Configuration [2]. The DMTF developed a set of standards for its WBEM architecture (Web Based Enterprise Management), including a data model, the Common Information Model (CIM) [3], an encoding specification, the xmlCIM Encoding Specification, and a transport mechanism, the CIM Operations over HTTP [4][5]. Upon CIM both organizations have specified new extensions namely the Policy Core Information Model (PCIM) [6].

A WBEM implementation typically includes four main components: a CIM server, or CIM Object Manager (CIMOM), a information repository, CIM clients and CIM providers. Figure 1 illustrates the WBEM architecture.

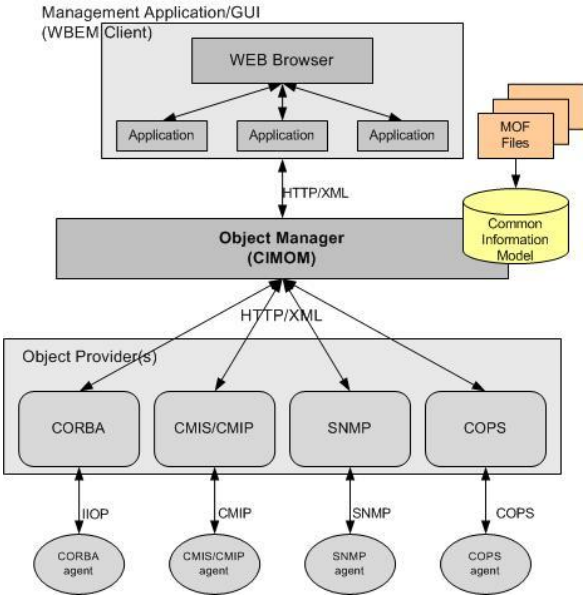

Figure 1 – WBEM architecture.

The CIMOM provides a repository where management clients can store or gather information about managed resources. Populating a CIMOM with data starts with importing or creating managed resource definitions in the CIMOM (about topology, resources, users,…). Descriptive files may be imported into the CIMOM, and subsequently instances of the classes that relate to a specific managed resource can be created within the CIMOM.

The management information is described in a specific language that was defined by the DMTF as a part of the overall WBEM specification – the Managed Object Format (MOF). It is a textual format language (both human and machine-readable) and it includes a Meta schema definition that defines the valid terms that are used to express a CIM schema and its usage. The data repository can be implemented in various ways (i.e. RDBMS, LDAP, XML,..).

CIM Clients and CIM providers act as managers and managed agents respectively.

3. The Daidalos project

Daidalos (**D**esigning **A**dvanced network **I**nterfaces for the **D**elivery and **A**dministration of **L**ocation independent, **O**ptimised personal **S**ervices) is an EU Sixth Framework Programme Integrated Project that aims at building a framework for the seamless integration of heterogeneous network technologies upon which users can enjoy a wide range of personalized services such as voice, data, and multimedia services [7].

The Daidalos network is divided in the three different parts: the Core Network (CN), the Access Network (AN), and Application Garden (AG), as it is illustrated in the Figure 2.

The CN is an IP network where resources are managed in an aggregated basis and it is supported by differentiated services [8]. It interconnects the access networks, the application gardens as well as the foreign domain networks. The connectivity between ANs and CN is realized through Edge Routers (ER). Inside the core network resource allocation is managed through a specialized entity – the Core Network QoS Broker (CNQoSBr). Besides QoS, several other management functions are being dealt by the following entities: Central Monitoring System (CMS), Authentication, Authorization, Accounting, Auditing and Charging System (A4C) and Multimedia Service Provisioning Platform (MSPP).

The AN resources are managed in a per-flow basis by a local QoS Broker (ANQoSBr). The AN topology may have several Access Routers (ARs), Core Routers (CRs) and Access Points (APs). The ANQoSBr has the responsibility for the AR and the CR configuration and management in order to grant QoS to the network clients. The ANQoSBr is also responsible for the admission control over the new packet flows in the AN; once a MT tries to establish a new session, the AR intercepts the session packets and requests the broker for the admission or rejection of the session. The ANQoSBr analyses the resource usage of its domain and returns the appropriate answer to the AR. The CNQoSBr can periodically update core network

resources parameters that are propagated to each edge router that assures the interface with ANs.

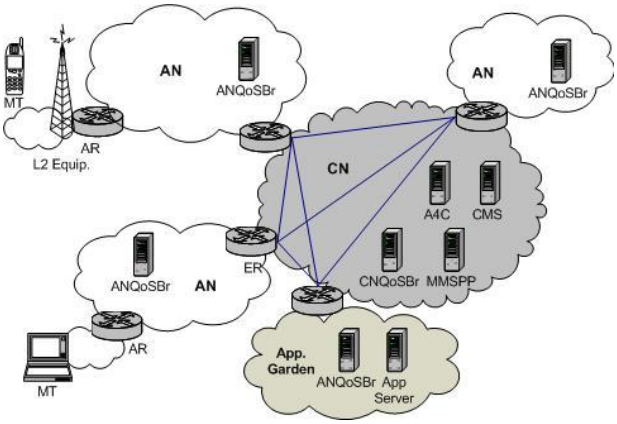

Figure 2 – Daidalos' Architecture.

The AG is a special case of an access network that supports application servers, service proxies and content adaptors, but not end users. These resources are managed as in a normal AN, according to the per-flow schema. The placement of the application servers and content adaptors apart from the core network has several advantages. It allows sharing a unique, and eventually more robust, security platform by all the servers inside the AG and it alleviates the CNQoSBr from the overload caused by the admission control of the servers' flows.

4. Daidalos PBNM architecture

Daidalos main goals are primary related with the achievement of technical solutions for mobile IP services, terminals and users. However, due to the inherent dependency on management issues, it was decided to consider the management architecture as an important factor for the success of the overall framework. In short, the PBNM system will have to manage and help to provide end-to-end QoS.

The main functionalities of the Policy-Based Network Management System (PBNMS) in Daidalos include:

- *Creating/editing/deleting rules and policies* – by using a UI (User Interface) it must be possible creation, edition and deletion of rules and policies. This element provides also immediate feedback when the network manager uses an improper syntax or enters incorrect data types (e.g. IP addresses when priorities are required).
- *Checking for policy conflicts and resolution* – since policies are based on a formalized, declarative specification of if-then rules, it is possible that the rules might be contradictory;
- *Storing policies* – the rules/policies are stored in a repository. This entity must maintain the integrity of the data it receives and stores, which means that any transaction that changes data must be completed and verified or else the affected data is restored, or rolled back, to its previous state;
- *Converting policies into commands* – the policy translation occurs from an abstract, high-level description, into low-level device configuration. The translation is necessary, because most network devices are unable to understand more abstract business-level concepts;
- *Distributing those commands to the network devices* – it is necessary to guarantee the distribution of the commands to the network devices in a reliable way;
- *Verifying policy distribution* – the necessity to notify the other components of the PBNMS of the success or failure of policies distribution and installation;
- *Monitoring and auditing* – monitoring is important to maintain the correct operation of the PBNMS. As new users and new applications are added, so it will be necessary to monitor how current policies can fit or not the operational requirements;

The PBNMS architecture is illustrated in Figure 3 and it follows closely the WBEM model.

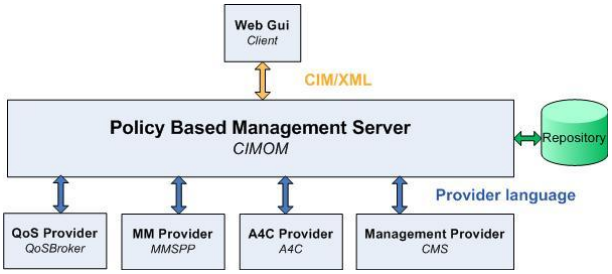

Figure 3 – PBNMS architecture.

At this stage of the project the PBNMS will provide interfaces for the following entities:

- *Authentication, Authorization, Accounting, Auditing and Charging server* (A4C) – it manages user information, authenticates the users, defines the services the user can have from the network, collects service usage information and controls charging information for network available services. Policies rules that affect services and users must be pushed into this system.

- *Access Network QoS Broker* (ANQoSBr) – it is responsible for the admission control and the management of the access network resource usage. Rules that depend on QoS parameters (bandwidth, jitter, delay) must be installed locally in the ANQoSBr.
- *Core QoS Broker* (CNQoSBroker) – manages core network resource usage. Its role is quite similar to the previous system.
- *Central Monitoring System* (CMS) – handles monitoring information. It activate probes (either passive or active), it collects monitoring data, processes it and sends the result to its clients (AnQoSBr for instance).
- *Multi Media Service Provision Platform* (MMSPP) – it contains several sub-entities like Content Servers, Content Adapters, Service Locator Servers and service proxies. Services catalogs can be available here so any rule that specifies restrictions for some kind of service must be propagated to this system.

The PBNMS is implemented upon a CIMOM server. The policies definitions are stored in the CIMOM repository, in a LDAP archive. The manager will define policies in a user application (CIMOM client) without going deep into technical details.

4.1. Policy engine

The policy engine is being implemented over a CIMOM open source implementation – OpenWBEM [9]. In order to decide about the CIMOM that better suits the Daidalos PBNMS needs, several open source systems were evaluated: OpenPegasus [10], OpenWBEM [9] and SBLIM [11]. Our choice was based on three main requirements: an active development/support community, a C++ developed solution and how general purpose is the management system. The OpenPegasus CIMOM was developed on C++ and is not a specific management solution, but it seems now very conservative concerning developments. Moreover, accordingly to a benchmark comparison [12], the OpenWBEM has better performance.

Using a CIM server to implement the PBNMS has several advantages: adaptation of CIMOM saves a lot of work because the policy server is already developed, it creates a very modular solution allowing distributing the PBNMS solution development by the project consortium partners without any extra effort, the solution is very interoperable because the communication with the CIMOM is performed in HTTP / CIM-XML, and, the final advantage is the fact that the project is making use of a solution already adopted by some industry members that could allow in the future some integration with commercial products.

The policy engine communicates with its clients or providers using the CIM-XML protocol, in which the policies are sent as CIM objects described in XML. Each policy entity uses a proper CIM provider to communicate with the CIMOM.

The use of a proper CIM provider to each type of client allows the customization of the provider accordingly to the client needs, as well as it allows to use a different communication protocol between the CIMOM and the different CIMOM clients. Typically, in Daidalos network, the user management entities implement the communication interfaces in Diameter or SAML, the QoS entities make use of the COPS protocol, and the multi-media server/proxy entities implement SIP interfaces. Having a proper provider for these types of entities allows the CIM server to interface with all of them.

4.2. Policy repository

All policies introduced by the operator will be stored in a global policy repository. The following assumptions regarding repository operation were done:

- the initial set of policies used to configure network entities are created by the network operator at the beginning of the network operation,
- the creation of new policies and changing of existing policies are made rarely (from a few minutes to months or years),
- the searching and reading of specific policies applied to particular entities is made often,
- the access to the repository should be based on the well known common protocol.
- in the repository a huge amount of information regarding e.g. network topology will be stored.

On the basis of the abovementioned assumptions it was decided to use X.500 directory service with Lightweight Directory Access Protocol (LDAP) for policy repository. LDAP directory servers are optimized for reading and searching operations. Additionally it is allowed to define an information schema which eases the exchanging of the information between different systems. The initial work regarding LDAP schema for the CIM Core Information Model as well as for CIM Extension Schema was already done by DMTF [13][14][15].

Beside of storing policies, LDAP repository is a good choice to store the information about users, services, configuration, and network entities. However,

the highly volatile information e.g. utilization of network links shouldn't be stored in LDAP repository.

The following CIM operations defined in [16] can be realized by LDAP repository:

- get a CIM Instance,
- delete a CIM Instance,
- modify a CIM Instance,
- enumerate instances of a CIM Class,
- enumerate instance names of a CIM Class,
- execute query,
- enumerate associators of a CIM Object,
- enumerate names of associators of a CIM Object,
- enumerate references to a CIM Object,
- enumerate names of references to a CIM Object,
- get a CIM Property value from a CIM Instance,
- set a CIM Property value from a CIM Instance.

In the PBNMS an LDAP module will be responsible for the translation of the abovementioned operations into the specific LDAP commands.

4.3. QoS provider

The QoS provider is the interface for the Daidalos QoS management entities: the ANQoSBr and the CNQoSBr. The interface is bidirectional: the QoS brokers will request the PBNMS for a configuration at startup time, and along the time it will send alarms/notifications to the PBNMS; the PBNMS will send a policy definition whenever it is (re)defined by the human operator or by automatic application triggers.

The QoS broker configuration information include the network topology description, the QoS description of the services offered by the operator, and the initial resource distribution that must be defined in its domain. The network topology information describes the ER, the CR and the ER list in terms of the available interfaces, the addresses, the available resources and the used technologies. The topology information describes as well the available AP's, their technology and the router interface to which they are connected. Using the topology information received from the PBNMS, the QoS broker should be able to determine the resources that are used by each service, as well as to decide if it can accept a new flow.

The services available are described by the PBNMS in terms of the DSCP code, the required resources both for the downlink and the uplink flows. It is very important for the operator to have a central network entity defining, in an integrated way, the service QoS parameters. A central service parameter definition avoids network configuration inconsistencies as well as it makes the configuration job much easier. Furthermore, when a service redefinition occurs the PBNMS performs an almost instantaneous QoS entities configuration.

The QoS network configuration is performed accordingly to the network usage. The broker can also use historical network usage information namely at start-up. The initial resource distribution is sent by the PBNMS. This is very important, especially in the CNQoSBr because, when it starts-up it should perform a CN resource distribution by all the AN's without any information of the resources normally needed by them.

4.4. CMS provider

In the Daidalos Network System the Real Time Monitoring System (RTMS) consists of two main types of entities:

1) The Network Monitoring Entities (NME) that are spread across the fixed network, located at strategic points. These elements may perform passive or active measurements.

2) The Central Monitoring System (CMS) which is responsible for controlling the measurement probes located in the fixed network. The CMS collects the results from the probes and analyses the information to put QoS and usage information into its central database. Collected information is made available to other Daidalos components for charging and billing purposes.

The CMS provides an interface between the PBNMS and the RTMS and acts as a Policy Decision Point (PDP) as well as a Policy Enforcement Point. Policies are distributed to the CMS as PCIM objects using CIM-XML.

The policies supported by the CMS falls into two main groups (Figure 4):

1) Configuration policies controlling the configuration of the monitoring system and the underlying probes. Policies in this group include policies for default configuration of probes activation/deactivation of probes, storing of test results and redirection of test results

2) Monitoring configuration and reporting policies, this group of policies allows the PBNMS to configure measurements and reporting schemes for the monitored network, including activation/deactivation of test, criteria for the evaluation of measurements and the actions to be taken when measurement results falls outside defined boundaries.

Once a new policy rule is pushed from the PBNMS to the CMS, the PBNMS interface component, in the CMS, will decide whether a measurement system must be established in order to evaluate when the condition

of the policy rule is being met. This means that one of the roles of the PBNMS-CMS interface component is to configure the CMS to set-up the relevant monitors for the policy rule. The PBNMS interface component uses the native CMS configuration for the configuration of the measurement tasks and probes.

If the policy contains an action condition that implies reporting of network events back to the PBNMS a specific interface component will subscribe to relevant measurement data, evaluate the data and issue triggers or events to the PBNMS.

To fulfill this task PBNMS interface component contains scanners that can retrieve measurement data from the CMS at regular intervals and issue events if certain conditions are fulfilled.

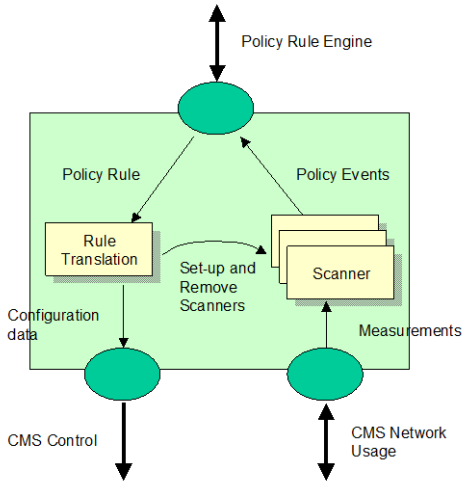

Figure 4 – CMS Provider.

5. Conclusion

During the precedent years network management paradigms have successively evolve to fit on a grown and highly mutable telecommunication market. Focus has shifted from basic device configuration and elementary FCAPS functionality towards a broader approach where management views the network as a whole and not as individual devices. This view has changed the network management paradigm and instead of low level "instrumentation" procedures the challenge is now the construction of high level management rules – policies – applicable to the whole network.

The number of entities evolved in the 4G operator operation as well as its diversity creates important challenges for the management activities. Managing a 4G operator requires that all entities evolved in a service offer are configured in a coherent manner. For instance service QoS definition should be coherent with the information present in the A4C server as well as it should be articulated with the monitoring information. A second requirement for a 4G management is an integrated configuration at the operator domain scope. For instance the service properties should be the same in the entire operator domain.

Policy-Based Network Management paradigm proposes an integrated management that answers the 4G management requirements.

In this paper we have evaluated several WBEM CIMOM in order to obtain a solid framework for the deployment of our PBNMS implementation. The OpenWBEM CIMOM was chosen based mainly of the maturity of this project. DEN-NG and SID, despite not being so solid solutions are being evaluated as possible migration models. Upon OpenWBEM, several components are being developed such as QoS providers, a CMS remote provider, LDAP repository, and providers for COPS and SNMP managed entities.

6. Acknowledgement

The work herein presented was developed in the scope of the DAIDALOS project (IST-2002-506997), funded by the European Community, under the Thematic Priority 'Information Society Technologies' of EU Framework Programme 6 for Research and Development.

7. References

[1] D. Durham et al., The COPS (Common Open Policy Service) Protocol, RFC2748, 2000.
[2] M. MacFaden et al., Configuring Networks and Devices with SNMP, RFC3512, 2003.
[3] DMTF, Common Information Model (CIM) Specification – Version 2.7. 2003.
[4] Thompson, J., Web-Based Enterprise Management Architecture. *IEEE Communications Magazine*, 1998. 36(3): p. 80-86.
[5] Web-Based Enterprise Management (WBEM) Initiative. 2004, Distributed Management Task Force, Inc.
[6] B. Moore, "Policy Core Information Model (PCIM) Extensions", RFC3460, 2003.
[7] Daidalos project, "Designing Advanced network Interfaces for the Delivery and Administration of Location independent, Optimised personal Services", (http://www.ist-daidalos.org)
[8] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss, "An Architecture for Differentiated Services", RFC 2475, IETF, December 1998.
[9] OpenWBEM project, (http://www.openwbem.org)
[10] Open Group, "C++ CIM/WBEM Manageability Services Broker" (http://www.openpegasus.com)

[11] SBIM Project, “SBLIM - Standards Based Linux Instrumentation for Manageability”, (http://www-124.ibm.com/sblim/index.html)
[12] Ying Zeng, Chris Hobbs, John Bell, Brian Quirt, “WBEM Server Benchmarks”, December 2003.
[13] DMTF, CIM Core Model v2.5, LDAP Mapping Specification, DSP0123, 2002.
[14] DMTF, LDAP Schema for the CIM v2.5 Physical Information Model, V1.0, DSP0124, 2001.
[15] DMTF, LDAP Schema for the CIM v2.5 User Information Model, DSP0121, 2001.
[16] DMTF, Specification for CIM operations over HTTP version 1.1, DSP0200, 2003.